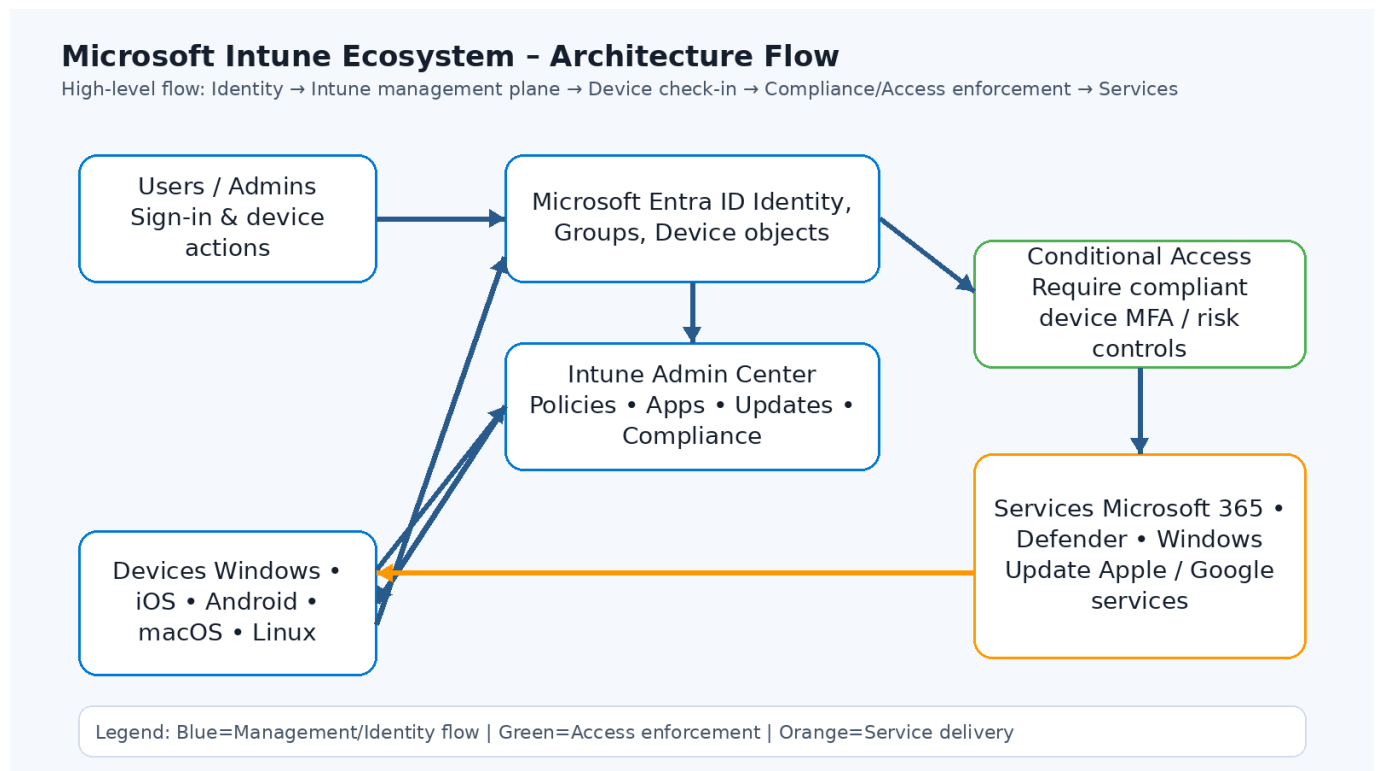


Microsoft Intune Deployment Guide: Optimization, Security & Best Practices

A practical, step-by-step reference for IT administrators to operationalize Intune after initial setup.



Tip: Use a pilot-first rollout model. Validate each change with a small group before broad deployment.

1. Optimize & Expand Your Environment

- Use Microsoft Entra ID dynamic groups to reduce manual targeting.
- Expand enrollment to iOS/Android (BYOD), macOS, and Linux where applicable.
- Integrate Conditional Access as the access enforcement layer.
- Standardize Windows provisioning with Windows Autopilot for zero-touch deployments.

Pro tip: Avoid rolling out to 'All Users' without pilot validation.

2. Windows Autopilot Deployment

- Register devices (OEM portal or hardware hash import).
- Create and assign an Autopilot deployment profile.
- User completes OOBE, signs in, and policies/apps apply automatically.
- Verify the device appears in Intune and is compliant.

3. Application Management

- Deploy business-critical apps as Required; optional apps as Available via Company Portal.
- Apply App Protection Policies (MAM) for BYOD scenarios.
- Monitor install status and investigate failures using device logs.

Warning: Stagger app deployments to reduce 'Pending install' backlogs.

4. Policy Enhancement

- Define compliance policies (OS version, encryption, antivirus, jailbreak/root detection).
- Use Settings Catalog for configuration profiles (modern approach).
- Deploy Microsoft Security Baselines and customize minimally.
- Review and resolve policy conflicts to prevent inconsistent outcomes.

5. Update & Patch Management

- Create update rings (pilot vs broad) with deferral and deadline policies.
- Control reboot behavior to reduce user disruption.
- Track update compliance via reports and exports.

Target: Aim for high security-update compliance within a defined SLA (e.g., 14 days).

6. Security & Access Control

- Require compliant devices for cloud-app access using Conditional Access.
- Enforce MFA—start with admin accounts and expand broadly.
- Integrate Microsoft Defender for Endpoint for risk signals and endpoint protection.

7. Monitoring & Health

- Use Intune dashboards and Endpoint Analytics to track health and performance.
- Create alerts for enrollment failures, expiring certificates, and compliance drops.
- Use remote actions (sync, restart, wipe) to remediate issues quickly.

8. Documentation & Training

- Maintain a living runbook: ownership, approvals, escalation, and change control.
- Train IT monthly; provide short end-user guides for Company Portal and MFA.
- Define support tiers (L1/L2/L3) to speed resolution.

9. Continuous Improvement

- Review assignments quarterly and remove stale groups.
- Run weekly compliance posture reviews.
- Test updates and app changes in a pilot group or test tenant.
- Collect user feedback and refine onboarding experience.

Quote: 'Intune is a journey, not a one-time setup.'

Next Steps

- Run an Autopilot pilot with a small set of devices.
- Create a dynamic group for Windows 11 devices and target baseline policies.
- Schedule a weekly compliance review and track exceptions.